(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2001 (31.05.2001)

PCT

(10) International Publication Number
WO 01/39428 A2

(51) International Patent Classification⁷: H04L 9/00

(21) International Application Number: PCT/US00/42241

(22) International Filing Date:
24 November 2000 (24.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/167,286	24 November 1999 (24.11.1999)	US
09/721,838	23 November 2000 (23.11.2000)	US

(71) Applicant: GEOPARTNERS RESEARCH, INC. [US/US]; 214 Lincoln Street, Suite 200, Boston, MA 02134 (US).

(72) Inventor: MOORE, James, F.; 27 Larchwood Drive, Cambridge, MA 02138 (US).

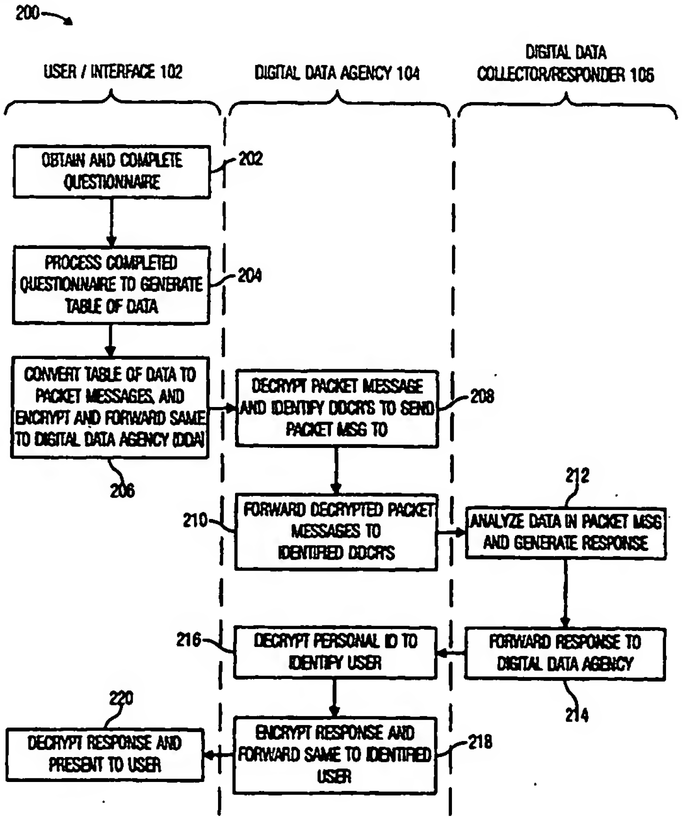
(74) Agents: CARR, Gregory, W. et al.; Carr & Storm, L.L.P., 900 Jackson Street, 670 Founders Square, Dallas, TX 75202 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR DISCLOSING PERSONAL DATA WHILE PROTECTING PERSONAL PRIVACY


200
USER / INTERFACE 102
DIGITAL DATA AGENCY 104
DIGITAL DATA COLLECTOR/RESPONDER 106
OBTAIN AND COMPLETE QUESTIONNAIRE
202
PROCESS COMPLETED QUESTIONNAIRE TO GENERATE TABLE OF DATA
204
CONVERT TABLE OF DATA TO PACKET MESSAGES, AND ENCRYPT AND FORWARD SAME TO DIGITAL DATA AGENCY (DDA)
206
DECRYPT PACKET MESSAGE AND IDENTIFY DDCR'S TO SEND PACKET MSG TO
208
210
FORWARD DECRYPTED PACKET MESSAGES TO IDENTIFIED DDCRS
212
ANALYZE DATA IN PACKET MSG AND GENERATE RESPONSE
216
DECRYPT PERSONAL ID TO IDENTIFY USER
FORWARD RESPONSE TO DIGITAL DATA AGENCY
214
220
DECRYPT RESPONSE AND PRESENT TO USER
ENCRYPT RESPONSE AND FORWARD SAME TO IDENTIFIED USER
218

(57) Abstract: A method for individuals to disclose personal data and enter into a mass-customized relationship with a web site, while protecting their personal privacy by affixing digital signatures and approvals-for-use to individual data items. The items are then sent to an intermediary site, referred to as a "digital data agency" that holds the personal data secure, but transmits the personal data to digital data collectors/responders (DDCRs) in accordance with permission provided by the user. Responses from the DDCRs are then sent to the DDA which encrypts the responses and forwards them to the user. The user may then decrypt the responses and review them.

IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR DISCLOSING PERSONAL DATA WHILE PROTECTING PERSONAL PRIVACY

TECHNICAL FIELD

The invention relates generally to the exposure of personal data and, more particularly, to a method and system that enables individual end users to voluntarily disclose personal data while protecting their personal privacy.

BACKGROUND

Periodically, individual persons will have a need to expose personal data about themselves to other parties such as, for example, marketers of products, providers of services such as health care or financial services, government agencies, other individual persons, and the like. In many cases, the individual wishes to make this data available only in the context of a particular transaction or relationship, or for a limited period of time, or until a specific event occurs. The individual may desire to provide specific permissions and restrictions for the use of such personal data, and prohibit non-approved uses. The individual may also desire prior, concurrent, or subsequent notification to himself or herself of the use or conveyance of each element of personal data conveyed to the other party.

By way of example, a person with a serious medical condition may desire to search and surf the web or visit chat rooms to find answers to issues regarding the medical condition, but the web and chat rooms are inefficient, and expose the person to significant privacy risks. Searching and surfing the web also exposes the user's keystrokes as the target of companies such as Engage™ that generate profiles based on a user's web behavior. At best this generates targeted banner ads that may or may not be desired, and at worst these profiles may be linked to the user's name and offline data. Chat rooms also require that the user provide his/her e-mail address or identity, which may invite undesired responses.

Thus, conventional technologies provide no practical method for managing an approval process that relates to collecting, storing, disseminating, and auditing the use of personal data.

On the other hand, so-called "anonymizer" or identity masking services, such as that provided by Zero-Knowledge Systems™, completely mask a user's identity to web sites, and make it impossible for sites to provide customized automated responses to particular users. Such systems conspicuously lack a technology that encourages the exchange of complex, conditional responses between a user and an automated website. What is needed is technology that integrates a privacy protection with enhancement of person-to-machine dialogue.

In addition to the foregoing, some governmental authorities, particularly several European governments and the European Community, have passed laws and regulations that require collectors of personal data to provide individuals with the ability to restrict the use of data about themselves, unless those individuals give specific approval in advance for its wider dissemination and use. At this time, though, there is no practical method for accomplishing this policy aim and complying with these laws.

The collectors of personal data about individuals, such as marketers of products, providers of services such as health care or financial services, government agencies, and the like, face substantial problems in responding to individuals. While they have the technical ability to create sites that are "mass customized" and communicate with a "unit of one" to customers, the collectors of data don't have sources of data and insight about customers that are reliable enough to drive such systems effectively. What they have is data that is partial, fragmentary, demographic and perhaps broadly psychographic, but that does not relate directly to things like customer values, intentions, and specific needs. This lack of data and insight is primarily due to the unwillingness of the customer to provide overt personal data, because of privacy concerns or lack of effective ways to do keep personal data private, and the resulting covert, unverified nature of the data that collectors have.

Moreover, even when collectors of personal data obtain valid data that generates useful insights, they cannot easily communicate with individuals in regard to elements of data. They collect increasing amounts of data without the approval of the individuals involved. They seek to use this data to create new value, but are increasingly either constrained by regulation or at risk of offending their customers if they use personal data in new ways without approval. On the other hand, there is no practical way for them to gain and manage such approval.

Thus, a need has arisen for methods and systems for protecting privacy while encouraging interaction between individuals and mass-customized, automated web services, and in the process gaining and managing approval from individuals for the collecting, storing, disseminating, and auditing the use of their personal data.

Such methods and systems should, among other things, also be effective for implementing the policy aim of, and complying with the laws of, governmental authorities, particularly European governments and the European Community, who have passed laws and regulations requiring collectors of personal data to provide individuals with the ability to restrict the use of data about themselves, unless those individuals give specific approval in advance for its wider dissemination and use.

SUMMARY

The present invention, accordingly, provides a method for enabling an individual end user to disclose personal data and enter into a mass-customized dialogue with one or more web sites, while protecting personal privacy. The method comprises steps performed by an individual end user to fill out questionnaires by way of a software application residing on the end user's computer or similar device, and generating packet messages containing encrypted personal data and an encrypted personal identifier of the user. The packet is sent to a digital data agency (DDA), which decrypts the personal date, but leaves the personal ID encrypted, and then forwards the packet messages to one or more digital data collector/responders (DDCR). The DDA then receives from the DDCRs responses to the packet messages, and decrypts the encrypted personal identifier to determine the individual end user. The DDA then encrypts the response, and forwards the encrypted response to an interface for review by the individual end user.

By the use of the present invention, personal data of individual persons may be collected, stored, disseminated, and audited in accordance with approvals and permissions provided by the individual. Data elements may also be processed individually (*i.e.*, element-by-element), thereby providing additional privacy to an individual. A user may also differentiate between data elements to provide different levels of protection for each data element. The transmission of data elements in packets also facilitates quick responses.

The present invention should, among other things, also be effective for implementing the policy aim of, and complying with the laws of, governmental authorities, particularly European governments and the European Community, who have passed laws and regulations requiring collectors of personal data to provide individuals with the ability to restrict the use of data about themselves, unless those individuals give specific approval in advance for its wider dissemination and use.

The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and the specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

FIGURE 1 is a high-level conceptual block diagram illustrating a system embodying features of the present invention;

FIGURE 1A exemplifies a questionnaire that may be used in connection with the system of FIG. 1;

FIGURE 2 is a flow chart illustrating steps executed on the system of FIG. 1 for practicing the present invention;

FIGURE 3 exemplifies entries made by a user for transmission to a digital data agency of FIG. 1; and

FIGURE 4 shows the structure of a data message sent by a user into the system of FIG. 1.

DETAILED DESCRIPTION

In the following discussion, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be obvious to those skilled in the art that the present invention may be practiced without such specific details. In other instances, well-known components have been illustrated in schematic or block diagram form in order not to obscure the present invention in unnecessary detail. Additionally, for the most part, and in the interest of conciseness, details concerning the Internet and the like have been omitted inasmuch as such details are not considered necessary to obtain a complete understanding of the present invention, and are within the skills of persons of ordinary skill in the relevant art.

It is further noted that, unless indicated otherwise, all functions described herein are performed by a processor such as computer or electronic data processor in accordance with code such as computer program code, software, or integrated circuits that are coded to perform certain functions.

Referring to FIGURE 1 of the drawings, the reference numeral 100 generally designates a system embodying features of the present invention that enables individual persons, *i.e.*, end users (not shown), to disclose personal data while protecting their personal privacy, by entering anonymously into mass-customized, automated dialogues of query and response with selected, preferably automated, web sites. The system 100 includes an interface 102, such as a computer terminal, personal digital assistant (PDA), or the like, through which an individual person (hereinafter "end user" or simply "user") or other provider of personal data may enter personal data. The interface 102 is connected in data communication with a digital data agency (DDA) 104 which acts in an intermediary role between the interface 102 and one or more audited, preferably automated, web sites, referred to herein as digital data collector/responders (DDCR) 106 (*e.g.*, a medical clinic), as discussed in further detail below.

The interface 102 further includes an applet 103 (small application program containing computer code) for execution on the interface 102 for enabling the user to enter personal data as discussed below. The interface 102 still further includes a registry 105, or access to an open, public registry, which contains a list of standard, generic questions, the answers to which would provide a DDCR 106 with sufficient information to enable it to be responsive to the needs of the user. The registry 105 also provides a data element registry number which is assigned to each question for purposes discussed below.

FIGURE 2 is a flowchart of steps executed in accordance with the present invention for disclosing a user's personal data while protecting the user's personal privacy. Prior to executing the steps shown in FIG. 2, a personal identity and a digital signature must be established in a public key encryption (*e.g.*, PGP) relationship between the user and the DDA 104. The DDA 104 may optionally request additional identifying information about the user, such as the user's home address, telephone number, and the like. Personal identities, digital signatures, encryption, and the like, are considered to be well-known in the art and, therefore, will not be discussed in further detail herein.

In step 202, the user obtains a suitable questionnaire from a suitable source, such as a DDCR 106 via the Internet, and completes it. For example, a person with Lupus may obtain a questionnaire to complete that would help him/her determine how he/she should deal with it. FIGURE 1A exemplifies a questionnaire 120 that a user may obtain. As shown, the questionnaire 120 requests that a user enter his/her personal ID in a blank 122, and then respond in blanks 124 to a number of corresponding questions that are relevant, for example, to dealing with Lupus. The questionnaire 120 then asks the user to fill in five approval/permission parameters 126, 128, 130, 132, and 134 relating to responses 124. In the parameter 126, a user identifies what use (*e.g.*, medical diagnostics) the responses 124 may be used for. The blank 128 requests that a user identify what uses (*e.g.*, an emergency referral to health a provider) other than those listed in the blank 126 a respective response 124 may be used for. In the parameter 130, the user identifies which parties (*e.g.*, web sites recognized by the user to be highly reliable sources of relevant information such as the Mayo Clinic, the National

Institute of Health, and Dr. Koop, and who operate mass-customized automated response capabilities in accordance with the present invention) the responses 124 may be disclosed to. In the parameter 132, a user identifies whether any parties, other than those identified in the parameter 130, may receive the responses 124. In the parameter 134, a user identifies a length of time (*e.g.*, three hours) that the approval/permission parameters 126, 128, 130, and 132 apply with respect to the responses 124. The questionnaire 120 may be customized in any of a number of different ways. For example, the parameters 126, 128, 130, 132, and 134 may be applied to each response 124 individually rather than as a group.

Upon completion of step 202, execution proceeds to step 204, wherein the completed questionnaire is processed by the applet 103 to generate a table 300 such as exemplified in FIGURE 3. As shown therein, the table 300 includes eight columns, or fields, 302, 304, 306, 308, 310, 312, 314, and 316, and any number of rows 314. The table 300 is generated based on the responses entered into the questionnaire 120 in step 202, and on data stored in the registry 105. Each row 314 corresponds to one response 124. More specifically, the user's personal ID 122 is encrypted and stored in the field 302. Each question corresponding to a respective response 124 is correlated through the registry 105 with a data element registry number, which is then entered into the field 304 of a respective row 314. The user's response 124 corresponding to the respective question, or data element registry number, is entered into the field 306 of a respective row 314. The fields 308, 310, 312, 314, and

316 correspond directly with the parameters 126, 128, 130, 132, and 134, respectively, for each respective response 124. For the questionnaire exemplified in FIG. 1A, the parameters 126, 128, 130, 132, and 134 would be the same for all rows 314. As mentioned above, however, the parameters 126, 128, 130, 132, and 134 may be individualized for each response 124, in which case the fields 308, 310, 312, 314, and 316 may differ for each row 314. The applet 105 then appends the user's aforementioned digital signature in a field 316. The user's e-mail reply address may be entered in the field 318 for facilitating further communications and notifications from the DDA 104 regarding the data entered in the table 300.

Upon completion of step 204, execution proceeds to step 206, wherein the applet 103 converts each row 314 of the table 300 of data to a packet message (also referred to as a "digital identity packet") 400, as depicted in FIGURE 4. Each packet message 400 contains eight fields 402, 404, 406, 408, 410, 412, 414, and 416 which correspond directly to each field 302, 304, 306, 308, 310, 312, 314, and 316, respectively, of a row 314 of the table 300. The fields 402, 404, 406, 408, 410, 412, 414, and 416 of each packet message 400 are then preferably encrypted (hence, the personal ID is preferably encrypted twice), and suitable headers (not shown) and the like, well-know in the art, are appended to the packet message for facilitating transmission of the packet message 400 to the DDA 104. The packet messages 400 are then transmitted from the interface 102 to the DDA 104.

In step 208, the DDA 104 receives and decrypts the packet messages 400 (hence rendering the personal ID still singly encrypted). The fields 412 and 414 of the decrypted packet messages 400 are then examined to identify the DDCRs 106 that should receive the packet messages 400. In step 210, the packet messages 400 are transmitted to the DDCRs identified in step 208. Prior to transmitting the packet messages 400 in step 210, the DDA 104 may optionally remove the fields 412 and 414 from the packet message 400. Alternatively, rather than transmitting the packet messages to DDCRs, thepacket messages may be made available for searching by the DDCRs, which may respond as desired.

In step 212, each DDCR 106 receives the packet messages 400 and analyzes the fields, namely, the fields 404 and 406, and from such analysis, generates an appropriate response. The DDCR 106 preferably utilizes rule-based software (*e.g.*, expert systems) to quickly generate responses to the packet messages. Each DDCR also notes and respects the use and time parameters identified in the fields 408, 410, and 416. The DDCR 106 may optionally also correlate the packet messages together based on the encrypted personal ID carried within the field 402 of each packet message to thereby perform a better analysis and generate a more meaningful response. It is noted, however, that the DDCR 106 is not enabled to decrypt the encrypted personal ID carried within the field 402 of the packet 400, but does include it in the response that it generates so that the DDA 104 may track the user to whom the response applies. In step 214, each DDCR 106 transmits the response generated in step 212, along with the encrypted personal ID carried within the field 402, to the DDAs 104 from which the DDCR received the packet messages 400.

In step 216, the DDA 104 receives the responses and associated encrypted personal ID from the DDCRs 106. The DDA 104 then decrypts the personal ID to identify the user that generated the packet messages to which the responses pertain. In step 218, the DDA 104 encrypts the response received from the DDCRs 106, and forwards the encrypted responses to the interface 102 of the identified user. In step 220, the interface 102 receives the encrypted messages and decrypts the responses. The interface 102 then presents the responses to the user in any conventional manner, such as via monitor or hardcopy.

By the use of the present invention, a method and system is provided by which personal data from individual persons may be collected, stored, disseminated, and audited in accordance with approvals and permissions provided by the individual. The use of the table 300 facilitates the handling of each individual data element (*e.g.*, the responses 124 and corresponding fields 304 and 306 of each row 314) with individual (*i.e.*, element-by-element) approvals and permissions. A user may thus differentiate between data elements to provide different levels of protection and approval for each data element. Each data element may also be processed individually, thereby providing additional privacy to an individual user. The transmission of data elements in packets 400 also facilitates quick responses.

The present invention should, among other things, also be effective for implementing the policy aim of, and complying with the laws of, governmental authorities, particularly European governments and the European Community, who have passed laws and regulations requiring collectors of personal data to provide individuals with the ability to restrict the use of data about themselves, unless those individuals give specific approval in advance for its wider dissemination and use.

It is understood that the present invention can take many forms and embodiments. Accordingly, several variations may be made in the foregoing without departing from the spirit or the scope of the invention. For example, should a DDCR 106, after it has provided a response, desire to provide additional responses in the future to an individual end user, the DDCR may query the intermediary DDA 104 to determine whether the individual would be willing to receive additional response. In a second example, the DDA 104 might query individual end users on its own behalf, to determine if they would be interested in receiving either questionnaires or responses from additional sites. In a third example, a particular DDCR 106 may offer to respond to questionnaires provided by other DDCRs, and could make this offer either by way of an intermediary DDA 104 or by mass appeals directly to potential end users (of course not knowing which or how many of the appeal group are current or past users of the system). In a fourth example, a DDCR's response to an individual end user may itself include an additional questionnaire, thus stimulating additional information-sharing by the end user, and providing more information for the DDCR to use in preparing subsequent responses.

Having thus described the present invention by reference to certain of its preferred embodiments, it is noted that the embodiments disclosed are illustrative rather than limiting in nature and that a wide range of variations, modifications, changes, and substitutions are contemplated in the foregoing disclosure and, in some instances, some features of the present invention may be employed without a corresponding use of the other features. Many such variations and modifications may be considered obvious and desirable by those skilled in the art based upon a review of the foregoing description of preferred embodiments. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

CLAIMS

1. A method for enabling a user to disclose personal data while protecting personal privacy, the method comprising the steps performed by an intermediary digital data agency of:

receiving at least one packet message containing personal data, including an encrypted personal identification (ID);

forwarding the at least one packet message to a digital data collector/responder (DDCR);

receiving from the DDCR a response to the packet message, the response including the encrypted personal ID;

decrypting the encrypted personal ID to identify the user that generated the at least one packet message;

encrypting the response received from the DDCR; and

forwarding the encrypted response to an interface for review by the user.

2. A method for enabling web sites to establish mass-customized, automated dialogues of query and response with an anonymous individual user, the method comprising the steps of:

providing a questionnaire to the user; and

the user entering into a mass-customized dialogue with the automated site, utilizing information and an encrypted identification (ID) supplied by the user in response to the questionnaire, and communicating by way of a trusted intermediary digital data agency (DDA).

3. A system for enabling a user to disclose personal data while protecting personal privacy, the system comprising:

a) an interface through which the user may enter personal data with encrypted personal identification (ID), and retrieve responses therefrom;

b) a digital data agency (DDA) coupled in data communication for receiving the personal data and encrypted personal ID from the interface; and

c) a digital data collector/responder coupled in data communication for receiving the personal data from the digital data agency, for generating a response to the personal data, and for transmitting the response to theDDA, which DDA forwards the response to the interface for retrieval by the user.

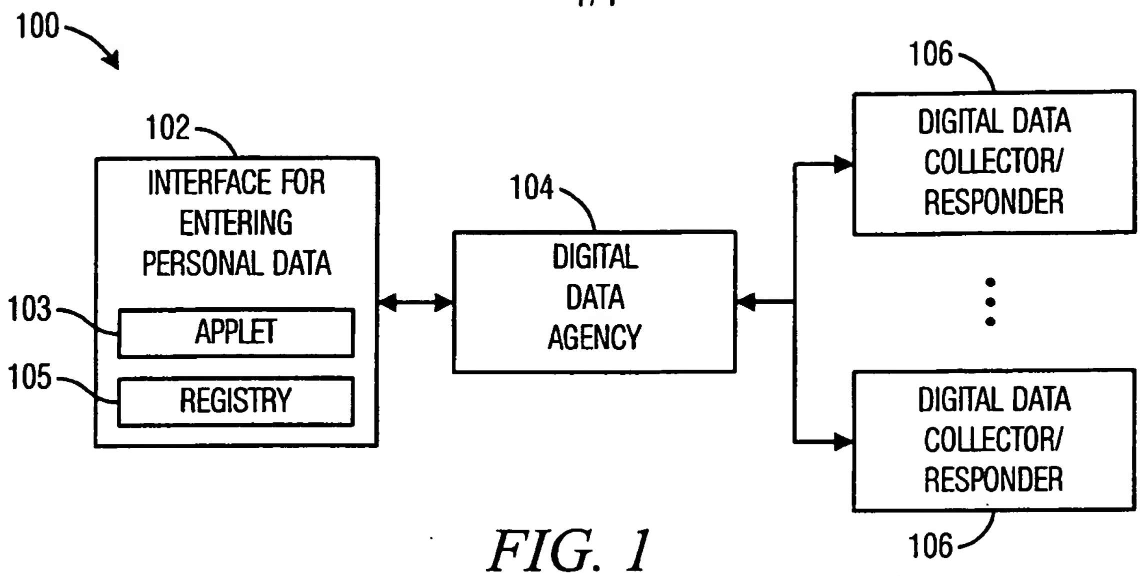

100
102
INTERFACE FOR ENTERING PERSONAL DATA
103
APPLET
105
REGISTRY
104
DIGITAL DATA AGENCY
106
DIGITAL DATA COLLECTOR/ RESPONDER
DIGITAL DATA COLLECTOR/ RESPONDER
106

FIG. 1

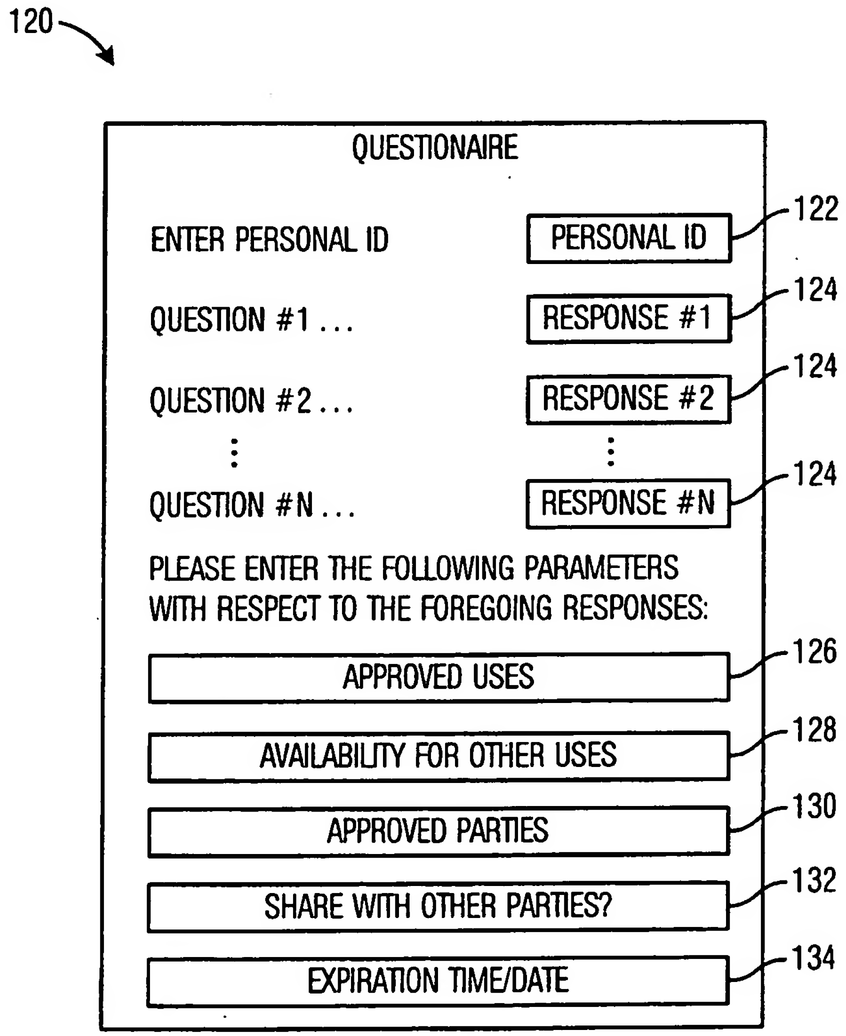

120
QUESTIONAIRE
ENTER PERSONAL ID
PERSONAL ID
122
QUESTION #1 . . .
RESPONSE #1
124
QUESTION #2 . . .
RESPONSE #2
124
QUESTION #N . . .
RESPONSE #N
124
PLEASE ENTER THE FOLLOWING PARAMETERS WITH RESPECT TO THE FOREGOING RESPONSES:
APPROVED USES
126
AVAILABILITY FOR OTHER USES
128
APPROVED PARTIES
130
SHARE WITH OTHER PARTIES?
132
EXPIRATION TIME/DATE
134

FIG. 1A

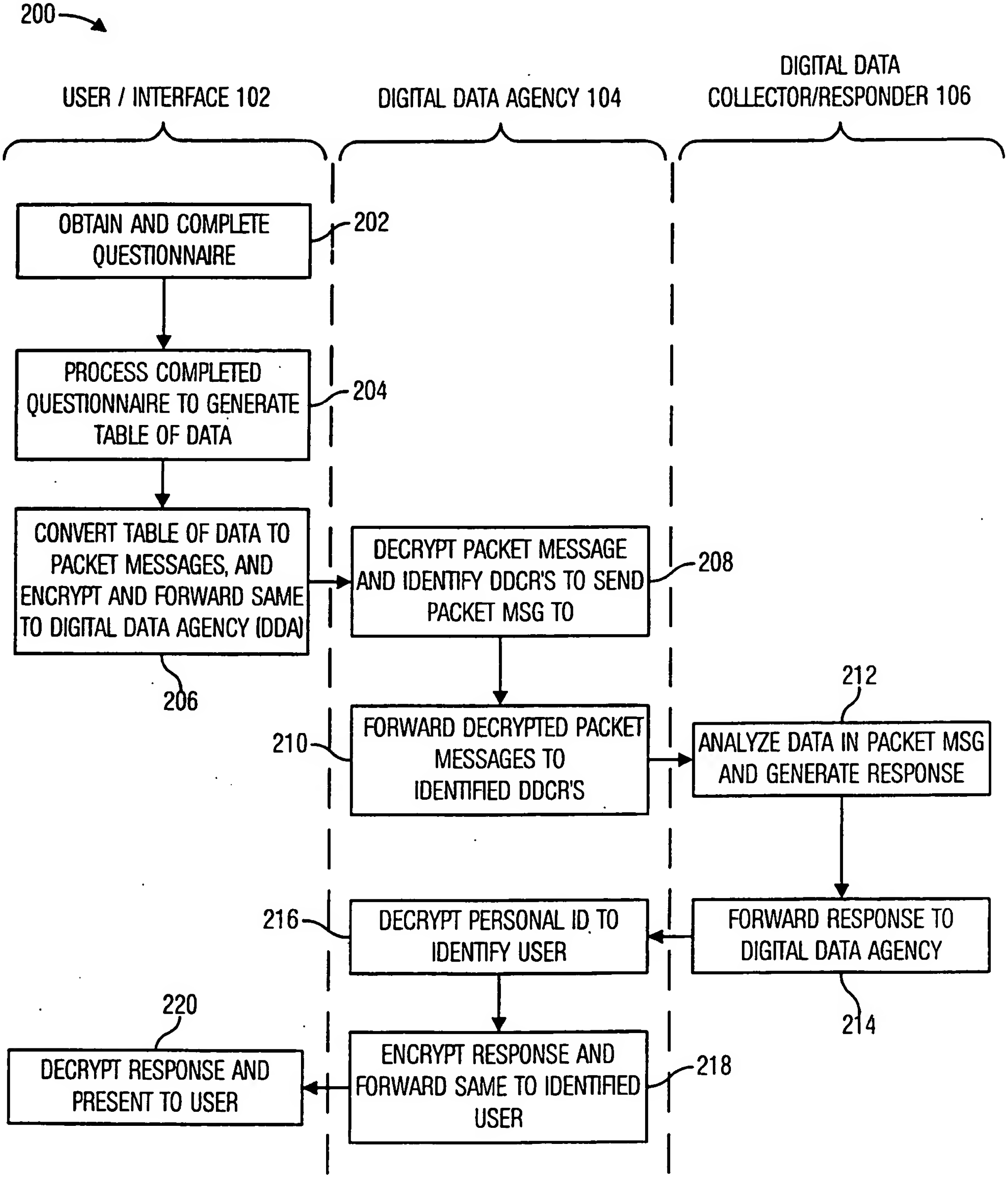

200
USER / INTERFACE 102
DIGITAL DATA AGENCY 104
DIGITAL DATA COLLECTOR/RESPONDER 106
OBTAIN AND COMPLETE QUESTIONNAIRE
202
PROCESS COMPLETED QUESTIONNAIRE TO GENERATE TABLE OF DATA
204
CONVERT TABLE OF DATA TO PACKET MESSAGES, AND ENCRYPT AND FORWARD SAME TO DIGITAL DATA AGENCY (DDA)
206
DECRYPT PACKET MESSAGE AND IDENTIFY DDCR'S TO SEND PACKET MSG TO
208
FORWARD DECRYPTED PACKET MESSAGES TO IDENTIFIED DDCR'S
210
ANALYZE DATA IN PACKET MSG AND GENERATE RESPONSE
212
FORWARD RESPONSE TO DIGITAL DATA AGENCY
214
DECRYPT PERSONAL ID TO IDENTIFY USER
216
ENCRYPT RESPONSE AND FORWARD SAME TO IDENTIFIED USER
218
DECRYPT RESPONSE AND PRESENT TO USER
220

FIG. 2

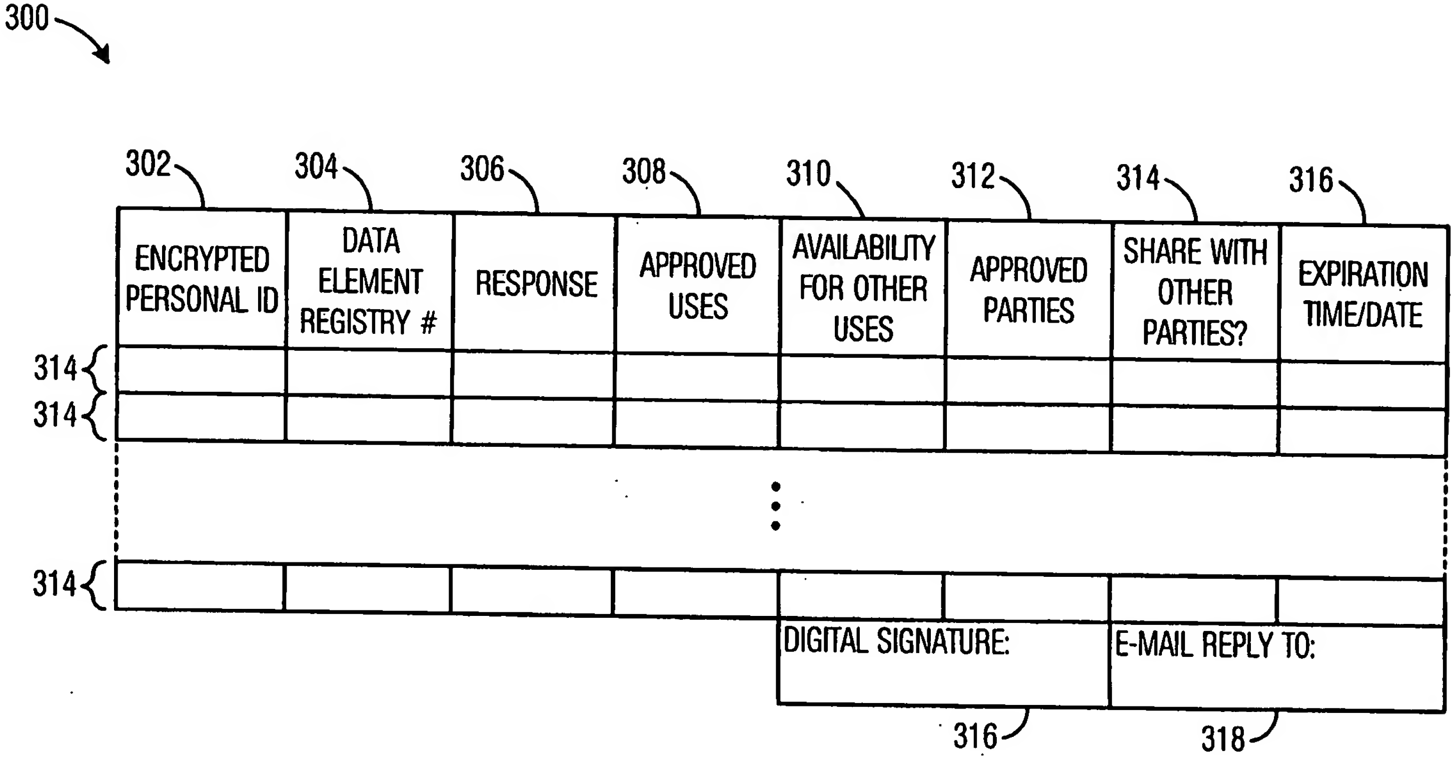

300
302
304
306
308
310
312
314
316
ENCRYPTED PERSONAL ID
DATA ELEMENT REGISTRY #
RESPONSE
APPROVED USES
AVAILABILITY FOR OTHER USES
APPROVED PARTIES
SHARE WITH OTHER PARTIES?
EXPIRATION TIME/DATE
314
314
314
DIGITAL SIGNATURE:
E-MAIL REPLY TO:
316
318

FIG. 3

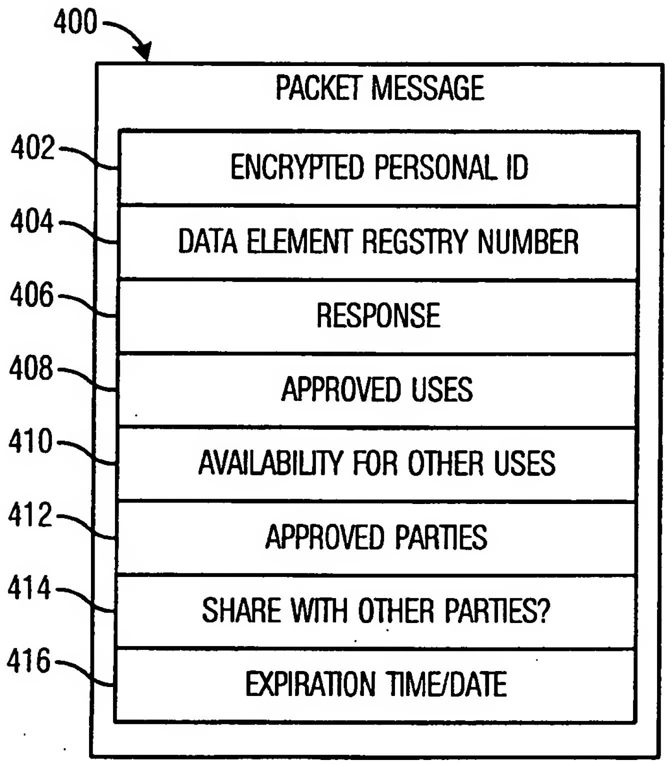

400
PACKET MESSAGE
402
ENCRYPTED PERSONAL ID
404
DATA ELEMENT REGSTRY NUMBER
406
RESPONSE
408
APPROVED USES
410
AVAILABILITY FOR OTHER USES
412
APPROVED PARTIES
414
SHARE WITH OTHER PARTIES?
416
EXPIRATION TIME/DATE

FIG. 4